(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 104205110 A
(43)申请公布日 2014.12.10

(21)申请号 201280071850.X

(22)申请日 2012.03.28

(85)PCT国际申请进入国家阶段日
2014.09.26

(86)PCT国际申请的申请数据
PCT/US2012/030861 2012.03.28

(87)PCT国际申请的公布数据
WO2013/147760 EN 2013.10.03

(71)申请人 英特尔公司
地址 美国加利福尼亚州

(72)发明人 S·阿户加 R·斯坦恩布瑞切
D·理查德森

(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 姬利永

(51)Int.Cl.
G06F 21/55(2013.01)

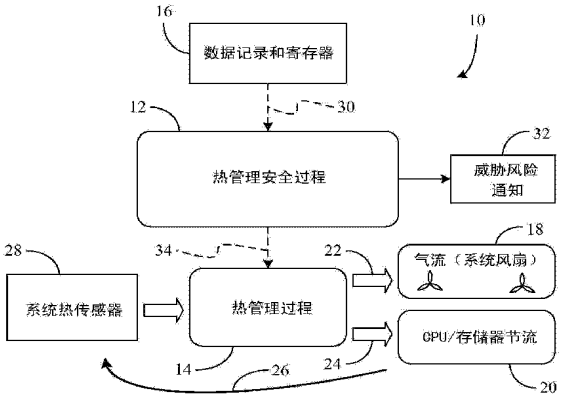
权利要求书2页 说明书4页 附图3页

(54)发明名称

保护固件中的热管理参数免受计算机攻击

(57)摘要

方法和系统可提供标识计算系统中的热管理设置以及将该热管理设置与有效配置信息进行比较。附加地，如果该热管理设置不符合该有效配置信息，修改该热管理设置，其中，该修改可致使该热管理设置符合该有效配置信息。附加地，可发起威胁风险通知，以便通知用户不符合。



CN 104205110 A

1. 一种计算机实施的方法，包括：

访问计算系统中的数据记录以及所述计算设置内的寄存器设置中的一个或多个，以标识热管理设置，其中，所述热管理设置包括风扇速度、传感器阈值、热偏移、以及强制节流状态中的一个或多个；

将所述热管理设置与有效配置信息进行比较；

如果所述热管理设置不符合所述有效配置信息，修改所述热管理设置，其中，修改所述热管理设置致使所述热管理设置符合所述有效配置信息；以及

通过系统事件日志条目和网络警报中的一个或多个发起威胁风险通知。

2. 如权利要求 1 所述的方法，进一步包括检测所述热管理设置的改变，其中，响应于所述改变标识所述热管理设置。

3. 如权利要求 1 所述的方法，进一步包括检测热节流条件，其中，响应于所述热节流条件标识所述热管理设置。

4. 如权利要求 1 所述的方法，其中，所述热管理设置被周期性地标识。

5. 一种系统，包括：

风扇；

温度传感器；

非易失性存储器，用于存储热管理设置；以及

逻辑，用于执行如权利要求 1 至 4 中任一项所述的方法。

6. 至少一种机器可读介质，包括多个指令，响应于在计算系统上被执行，所述指令致使所述计算系统执行根据如权利要求 1 至 4 中任一项所述的方法。

7. 一种计算机实施的方法，包括：

标识计算系统中的热管理设置；

将所述热管理设置与有效配置信息进行比较；以及

如果所述热管理设置不符合所述有效配置信息，修改所述热管理设置。

8. 如权利要求 7 所述的方法，其中，修改所述热管理设置致使所述热管理设置符合所述有效配置信息。

9. 如权利要求 7 所述的方法，其中，所述热管理设置包括风扇速度、传感器阈值、热偏移、以及强制节流状态中的一个或多个。

10. 如权利要求 7 所述的方法，其中，标识所述热管理设置包括访问数据记录和寄存器设置中的一个或多个。

11. 如权利要求 7 所述的方法，进一步包括通过系统事件日志条目和网络警报中的一个或多个发起威胁风险通知。

12. 如权利要求 7 所述的方法，进一步包括检测所述热管理设置的改变，其中，响应于所述改变标识所述热管理设置。

13. 如权利要求 7 所述的方法，进一步包括检测热节流条件，其中，响应于所述热节流条件标识所述热管理设置。

14. 如权利要求 7 所述的方法，其中，所述热管理设置被周期性地标识。

15. 一种系统，包括：

风扇；

温度传感器；

非易失性存储器，用于存储热管理设置；以及

逻辑，用于执行如权利要求 7 至 14 中任一项所述的方法。

16. 至少一种机器可读介质，包括多个指令，响应于在计算系统上被执行，所述指令致使所述计算系统执行根据权利要求 7 至 14 中任一项所述的方法。

保护固件中的热管理参数免受计算机攻击

[0001] 背景

技术领域

[0002] 实施例总体上涉及计算系统中的热管理。更具体地，实施例涉及保护热管理参数免受计算机攻击。

[0003] 讨论

[0004] 常规的计算系统可包括使用热管理参数来控制风扇和节流存储器、处理器等等的固件，其中，热管理参数可易受攻击。例如，黑客可发布将高风扇速度和低风扇速度设置成零的命令，这可基本上在所有情况下关闭风扇。实际上，这种攻击可致使系统关机以及对系统的组件造成永久损坏。而且，数据中心操作员可能未察觉到就位的热控制技术的硬件 / BIOS（基本输入输出系统）或固件细节。因此，可需要相当大的时间量从攻击恢复。

[0005] 附图简要说明

[0006] 通过阅读以下说明书和所附权利要求书并且通过参考以下附图，本发明实施例的各种优点将对本领域普通技术人员变得明显，在附图中：

[0007] 图 1 是根据实施例的具有热管理安全过程的架构的示例的框图；

[0008] 图 2 是根据实施例的保护热管理参数免受攻击的方法的示例的流程图；以及

[0009] 图 3 是根据实施例的计算系统的示例的框图。

[0010] 详细描述

[0011] 现在转向图 1，示出了架构 10，其中热管理安全过程 12 被布置在热管理过程 14 和由热管理过程 14 用于控制计算系统中的气流组件 18 和 / 或节流组件 20 的一个或多个数据记录和寄存器 16 之间。计算系统可包括例如服务器、个人计算机 (PC)、个人数字助理 (PDA)、笔记本计算机 / 上网本计算机、桌上计算机、智能平板计算机、无线智能电话、媒体播放器、智能电视、移动互联网设备 (MID) 等等。具体而言，数据记录和寄存器 16 可包括包含计算系统的热管理参数（诸如风扇速度、传感器阈值、热偏移、强制节流状态等等）的用户可配置传感器数据记录 (SDR)、芯片组寄存器等等。因此，所示出的热管理过程 14 向气流组件 18 发布风扇控制输出 22（例如，脉宽调制 /PWM 信号）以及向节流组件 20 发布节流相关输出（例如，存储器热偏移值、强制节流信号），以便实现在反馈环路中由计算系统的一个或多个热传感器 28 所检测的冷却结果 26。

[0012] 如将更详细地讨论的，安全过程 12 可将从数据记录和寄存器 16 检索的“不合格”热管理参数 30 与有效配置信息进行比较，并且如果其不符合有效配置信息则修改热管理参数。有效配置信息可指定例如哪些范围的 SDR 风扇控制数据被认为是可接受的以及哪些被认为是不可接受的（例如，可导致系统过热以及随后关机的设置）。有效配置信息可以是被数字地签名并且仅通过向计算系统加载不同的控制器固件图像可修改的控制器固件图像的一部分。因为该图像是签名的，可用这种方法保证其来源和真实性。

[0013] 如果不合格热管理参数 30 不符合有效配置信息，所示出的安全过程 12 生成热风险通知 32 并且修改热管理参数，从而使得其符合有效配置信息。如果不合格热管理参数 30

已经符合有效配置信息，其可被未修改地传递到热管理过程 14。在任一个实例中，在所示出的示例中，热管理过程 14 被提供有“合格”热管理参数 34。可通过周期性地（例如，每五秒）检测热管理参数和 / 或热节流条件（例如，过量节流、持久性过低风扇速度）等等或其组合的改变来触发安全过程 12。

[0014] 图 2 示出保护热管理参数免受攻击的方法 36。方法 36 可被实现为存储在至少一个机器或计算机可读存储介质（诸如随机存取存储器 (RAM)、只读存储器 (ROM)、可编程 ROM(PROM)、闪存、固件、微代码等等）中、在可配置逻辑（诸如可编程逻辑阵列 (PLA)、现场可编程门阵列 (FPGA)、复杂可编程逻辑器件 (CPLD)）中、在使用电路技术（诸如专用集成电路 (ASIC)、互补金属氧化物半导体 (CMOS) 或晶体管 - 晶体管逻辑 (TTL) 技术或其任意组合）的固定功能硬件中的可执行逻辑指令集。例如，可用一种或多种编程语言的任意组合编写用于执行方法 36 中所示的操作的计算机程序代码，包括面向对象的编程语言，诸如 C++ 等等，以及常规程序编程语言，诸如“C”编程语言或类似的编程语言。而且，可使用任意上述电路技术将方法 36 的各个方面实现为处理器的嵌入逻辑。

[0015] 所示出的处理框 38 确定计算系统的一个或多个热管理设置是否已经改变。如果未改变，框 40 可确定是否存在节流条件（诸如处理器和 / 或存储器设备的过量节流）。如果不存在这种条件，可在框 42 确定预定时间段是否过期。如果热管理设置已经改变，则存在节流条件，或者预定时间段已过期，所示出的框 44 标识一个或多个不合格热管理设置，其中，可在框 46 将不合格热管理设置与有效配置信息进行比较。如果在框 48 确定不合格热管理设置不符合有效配置信息，框 50 可修改不符合的热管理设置，从而使得它们符合。因此，例如，在框 50 的修改可涉及重置风扇速度、传感器阈值和 / 或热偏移、将计算系统的组件设置在节流状态（或反之亦然）等等。所示出的框 52 提供通过例如创建系统事件日志 (SEL) 条目和 / 或网络警报来发起威胁风险通知。

[0016] 现在转向图 3，示出计算系统 54。所示出的计算系统 54 可包括例如服务器、PC、PDA、笔记本计算机 / 上网本计算机、桌上计算机、智能平板计算机、无线智能电话、媒体播放器、智能电视、MID 等等或其组合。该计算系统可总体上包括各温度传感器，以便检测过热，其中，可通过控制风扇 56 和 / 或节流发热组件来解决过热。例如，一个或多个中央处理单元 (CPU)58、互连（诸如“南桥”芯片 62）、电源 66、系统存储器 70、网络接口控制器 (NIC)74、前板 76、存储后板 78 以及一个或多个输入 / 输出 (IO) 竖板 (riser)79 可全部配备有能捕获与计算系统 54 的操作相关的热数据。而且，一个或多个离散温度传感器 80 可获得热测量值，其中，热数据可用于冷却反馈环路中，如已经讨论的。附加的，CPU 和 / 或南桥内部逻辑（诸如管理引擎 82）可用于进行节流活动，以便将计算系统 54 维持在可接受的热操作点和 / 或限制系统功耗。

[0017] 所示出的计算系统 54 还包括控制器 84，诸如具有逻辑 86 的基板管理控制器 (BMC)，该逻辑被配置用于：标识计算系统 54 中的热管理设置；将热管理设置与有效配置信息进行比较；如果热管理设置不符合有效配置信息则修改热管理设置；以及通过例如存储在非易失性存储器 (NVM)88、NIC 74（例如，网络警报）、前板 76、和 / 或一个或多个故障发光二极管 (LED)92 中的 SEL 条目发起威胁风险通知。热管理设置的修改可致使热管理设置符合有效配置信息。

[0018] 在一个示例中，逻辑 86 可从存储在 NVM 88 中的 SDR 或者从计算系统 54 中的其他

寄存器检索热管理设置。在所示出的示例中，控制器 84 包括专用 RAM 90，其中，RAM 90 和系统存储器 70 可包括例如双倍数据率 (DDR) 同步动态 RAM(SDRAM，例如，DDR3SDRAM JEDEC 标准 JESD79-3C，2008 年 4 月）模块。系统存储器 76 和 / 或控制器 RAM 90 的模块可被结合到单个内联存储器模块 (SIMM)、双内联存储器模块 (DIMM)、小型外联 DIMM(SODIMM) 等等中。在一个示例中，系统存储器 70 是计算系统 54 的操作过程中的显著热量的潜在来源。

[0019] 所示出的 CPU 58 可包括一个或多个处理器核（未示出）以便执行与主机 OS（操作系统）和 / 或应用软件相关联的一个或多个驱动器，其中，每个核可以通过指令提取单元、指令解码器、一级 (L1) 高速缓存、执行单元等等来完善功能。在一个示例中，CPU 58 是计算系统 54 的操作过程中的显著热量的潜在来源。

[0020] NIC 74 可提供离平台通信功能，用于各种各样的目的，诸如例如蜂窝电话（例如，W-CDMA(UMTS)、CDMA2000(IS-856/IS-2000) 等等）、Wi-Fi（无线保真，例如电气与电子工程师协会 /IEEE 802.11-2007、无线局域网 /LAN 媒体接入控制 (MAC) 以及物理层 (PHY) 规范）、蓝牙（例如，IEEE 802.15.1-2005、无线个域网）、WiMax（例如，IEEE 802.16-2004、LAN/MAN 宽带无线 LAN)、全球定位系统 (GPS)、扩展频谱（例如，900MHz)、以及其他 RF（射频）电话目的。在一个示例中，NIC 74 是计算系统 54 的操作过程中的显著热量的潜在来源。

[0021] 实施例因此可提供其中标识计算系统中的热管理设置的计算机实施的方法。该方法可提供将热管理设置与有效配置信息进行比较以及如果热管理设置不符合有效配置信息则修改热管理设置。

[0022] 实施例还可包括具有风扇、温度传感器、用于存储热管理设置的非易失性存储器、以及用于标识热管理设置的逻辑的计算系统。附加地，该逻辑可将热管理设置与有效配置信息进行比较以及如果热管理设置不符合有效配置信息则修改热管理设置。

[0023] 附加地，实施例可包括包含指令集的至少一个计算机可读存储介质，如果被处理器执行，该指令集可致使计算系统标识计算系统内的热管理设置。指令还可致使计算系统将热管理设置与有效配置信息进行比较以及如果热管理设置不符合有效配置信息则修改热管理设置。

[0024] 其他实施例可提供其中访问计算系统内的数据记录和计算系统内的寄存器设置中的一个或多个以便标识热管理设置的计算机实施的方法。热管理设置可包括风扇速度、传感器阈值、热偏移、以及强制节流状态中的一个或多个。该方法还可提供将热管理设置与有效配置信息进行比较以及如果热管理设置不符合有效配置信息则修改热管理设置，其中，修改热管理设置致使热管理设置符合有效配置信息。附加地，通过系统事件日志条目和网络警报中的一个或多个发起威胁风险通知。

[0025] 可使用硬件、软件、或其组合并且可在一个或多个计算机系统或其他处理系统中实现本发明实施例的某些方面。可将程序代码应用到使用输入设备输入的数据，以便执行所描述的功能并且生成输出信息。输出信息可被应用到一个或多个输出设备。本领域普通技术人员可认识到实施例可在不同的计算机系统配置下实践，包括多处理器系统、微型计算机、大型计算机等等。实施例还可在分布式计算系统中实践，其中可由通过通信网络链接的远程处理设备执行任务。

[0026] 每个程序可被实现在高级程序或面向对象的编程语言中，以便与处理系统通信。

然而，程序可被实现在汇编或机器语言中，如果希望的话。在任何情况下，语言可以是功能性的、被编译的或被解释的。

[0027] 程序指令可用于致使使用指令编程的通用或专用处理系统执行在此所描述的方法。可替代地，可由包含用于执行该方法的特定硬接线逻辑或由编程计算机组件和定制硬件组件的任何组合来执行该方法。在此所述的方法可被提供为计算机程序产品，该计算机程序产品可包括其上存储有指令的至少一个机器可读介质，该指令可用于对处理系统或其他电子设备进行编程，以便执行该方法。在此所使用的术语“机器可读介质”或“机器可访问介质”应当包括能够存储或编码指令序列以便由机器执行的并且致使机器执行在此所述的任何一种方法的任何介质。术语“机器可读介质”或“机器可访问介质”可因此包括但不限于对数据信号进行编码的固态存储器、光盘和磁盘、以及载波。而且，本领域常常见的是当采取行动或造成结果时谈及一种或另一种形式的软件（例如，程序、过程、进程、应用、模块、逻辑等等）。这种表达仅仅是表述通过处理系统执行软件以便致使处理器执行动作或产生结果的简化方式。

[0028] 术语“耦合”可在此用于指代有关组件之间的任何类型的关系（直接的或间接的）并且可应用到电、机械、流体、光、电磁、机电或其他连接。附加地，术语“第一”、“第二”等等可在此仅用于方便讨论并且不带有任何特定的时间或时间顺序的意义，除非另外指明。

[0029] 尽管已经在以上描述本发明的不同实施例，应当理解的是已经通过举例而非限制展现了它们。本领域普通技术人员将理解的是可在不背离如在所附权利要求书中所定义的本发明的精神和范围的情况下做出各种形式和细节的改变。因此，本发明的幅度和范围不应当受限于上述示例性实施例，而是应当根据以下权利要求书及其等效方案来定义。

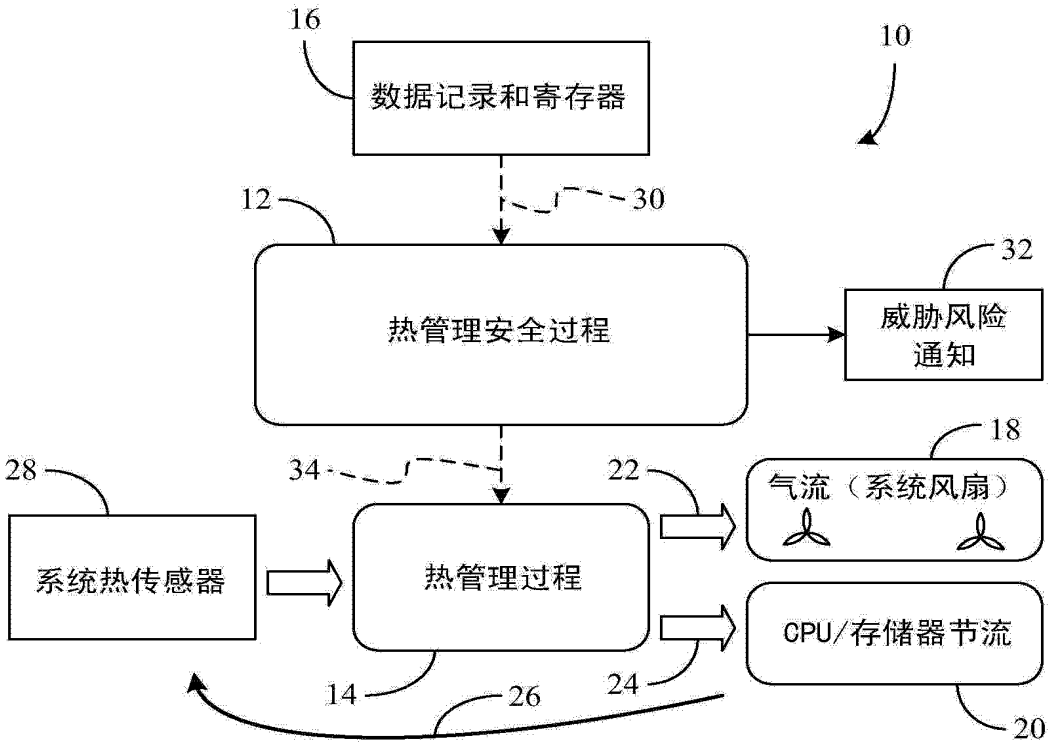

16
数据记录和寄存器
10
12
30
热管理安全过程
32
威胁风险
通知
18
28
34
22
气流（系统风扇）
系统热传感器
热管理过程
CPU/存储器节流
14
26
24
20

图 1

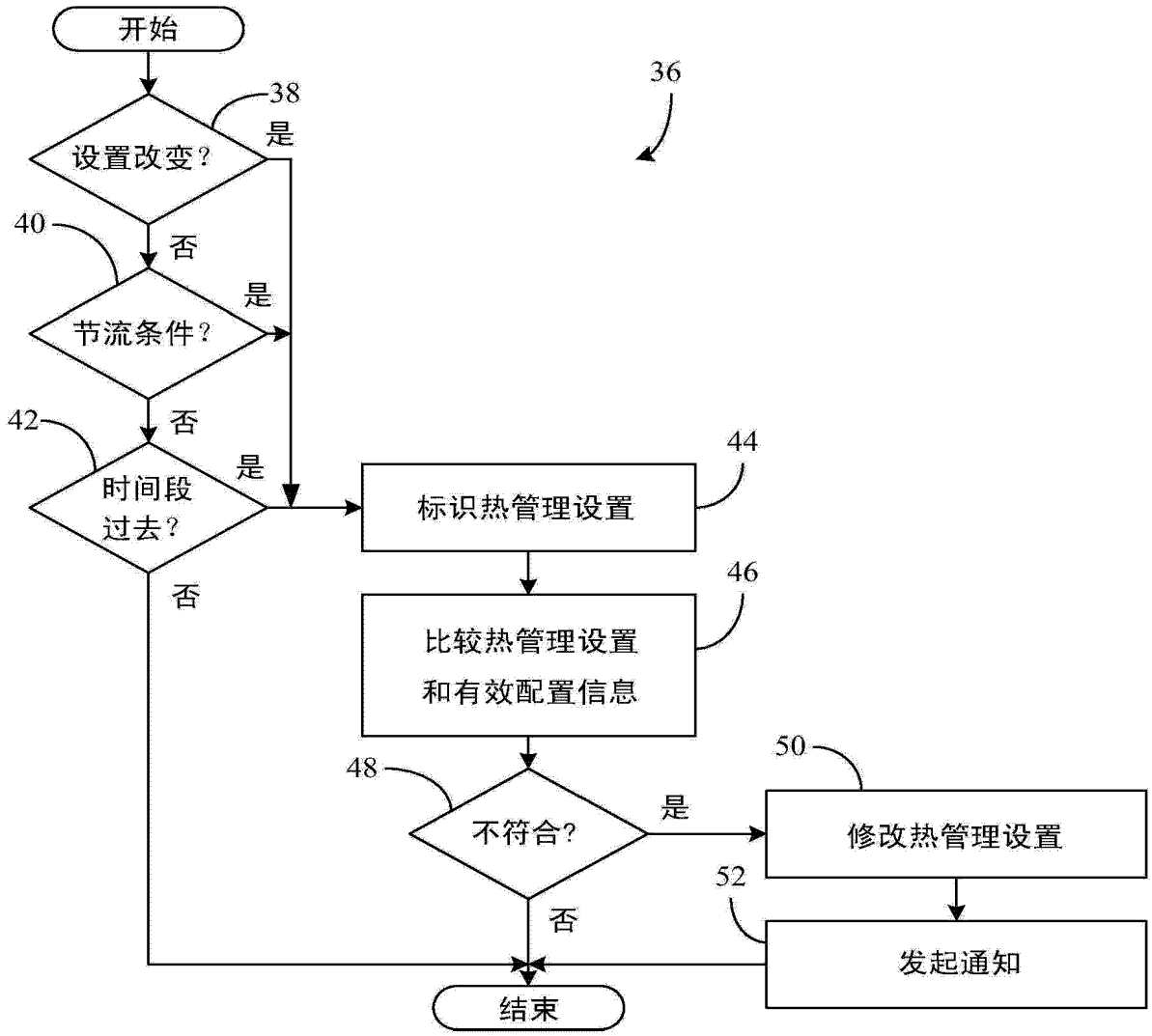


图 2

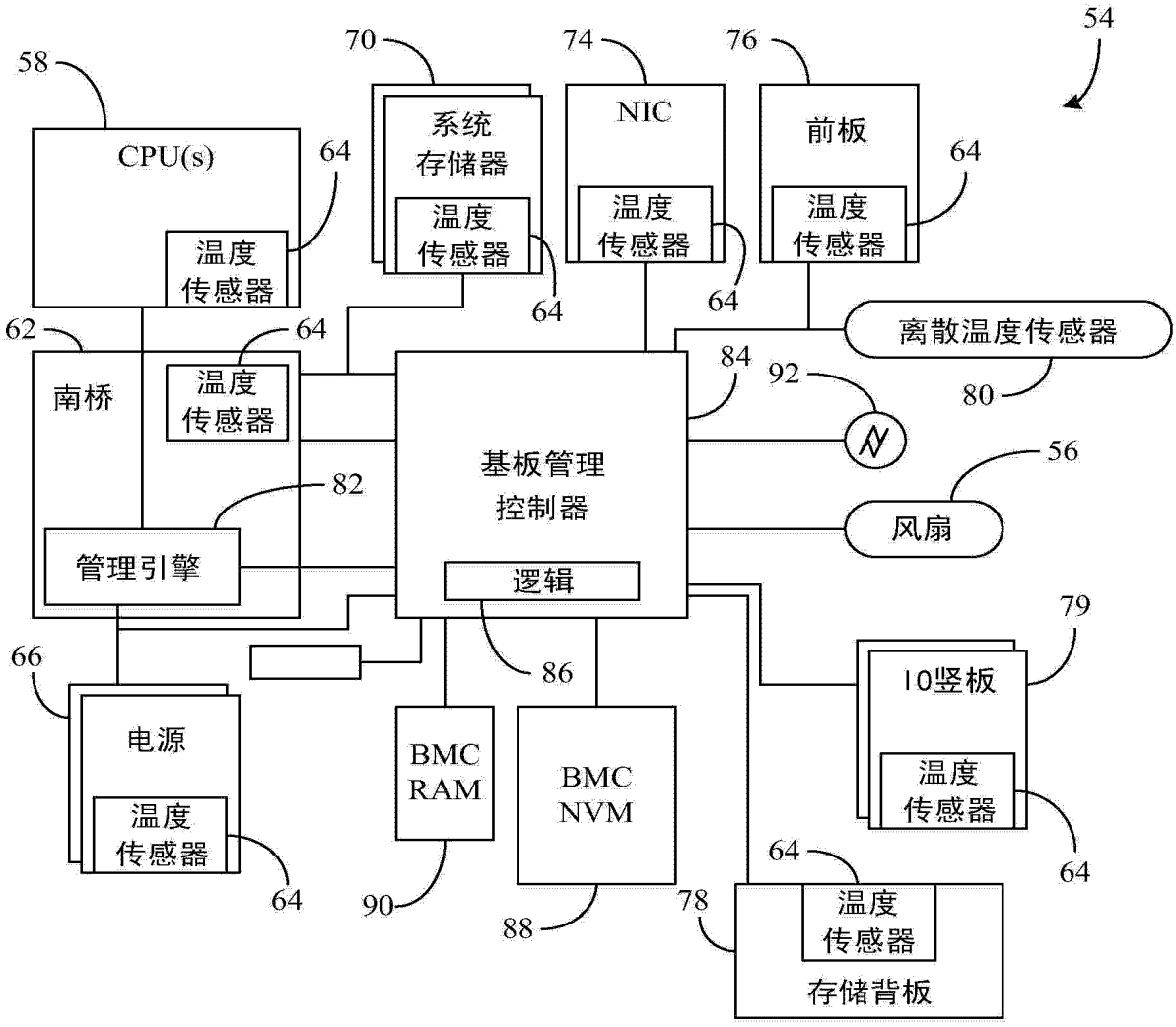

54
58
70
74
76
CPU(s)
64
系统
存储器
温度
传感器
NIC
温度
传感器
前板
温度
传感器
64
64
64
62
64
离散温度传感器
南桥
温度
传感器
84
92
80
基板管理
控制器
56
82
风扇
管理引擎
逻辑
79
66
86
IO竖板
电源
温度
传感器
BMC
RAM
BMC
NVM
温度
传感器
64
64
90
88
78
64
温度
传感器
存储背板

图 3